Number Theory Section Summary: 4.4
Linear Congruences

1. Summary

Recall that a **congruence** is an equation of the form $P(x) \equiv 0 (\text{mod } n)$; a **linear congruence** should be that equation with $P(x) = ax - b -$ and it is!

$$ax - b \equiv 0 (\text{mod } n) \iff ax \equiv b (\text{mod } n)$$

which means that $ax - b = ny$ for some $y \in \mathbb{Z}$; rewriting, we have that

$$ax - ny = b$$

to be solved in integers – that is, a Diophantine equation!

Now the Diophantine equation could have an infinite number of solutions, but since we're working modulo n, we're only interested in solutions distinct mod n.

2. Definitions

linear congruence a congruence in which $P(x)$ is of the form $P(x) = ax - b$.

3. Theorems

Theorem 4.7: The linear congruence $ax \equiv b (\text{mod } n)$ has a solution if and only if $d|b$, where $d = \gcd(a, n)$. If $d|b$, then the linear congruence has d mutually incongruent solutions modulo n.

Example: #1bdf, p. 82 Solve the following linear congruences:

- $5x \equiv 2 (\text{mod } 26)$

$$\overset{1}{5} \cdot 5x \equiv 5 \cdot 2 (\text{mod } 26)$$
$$25x \equiv 10 (\text{mod } 26)$$
$$-x \equiv 10 (\text{mod } 26)$$
$$x \equiv -10 (\text{mod } 26)$$
$$x \equiv 16 (\text{mod } 26)$$

- $36x \equiv 8 \pmod{102}$ (no solution - check gcd first!)
- $140x \equiv 133 \pmod{301}$

[Hint: $\gcd(140, 301) = 7$] "Divide by 7":

4. Properties/Tricks/Hints/Etc.

$7 \cdot 20x \equiv 7 \cdot 19 \pmod{301}$

by Theorem 4.3 (1) 67

$20x \equiv 19 \pmod{43}$

(Observe that 301, a multiple of 43, is 1 off a multiple of 20 - so choose to multiply the equation by 15)

$300x \equiv 15 \cdot 19 \pmod{43}$

$-x \equiv 285 \pmod{43}$

$-x \equiv -16 \pmod{43}$

$x \equiv 16 \pmod{43}$

The rest of the solutions are obtained by adding multiples of 43 - these will be distinct (incongruent) modulo 301....